

PORTABLE SIGNAL PROCESSOR

Publication number: JP2000194799

Publication date: 2000-07-14

Inventor: YAMADA MASANARI; SHIBATA NAOITO

Applicant: DAINIPPON PRINTING CO LTD

Classification:

- **international:** G06K19/07; G06K17/00; G06K19/07; G06K17/00;
(IPC1-7): G06K17/00; G06K19/07

- **European:**

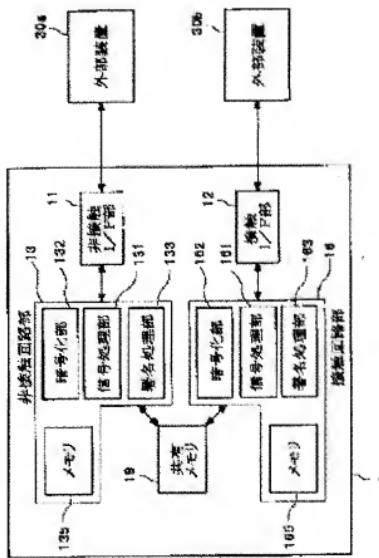
Application number: JP19980368157 19981224

Priority number(s): JP19980368157 19981224

[Report a data error here](#)

Abstract of JP2000194799

PROBLEM TO BE SOLVED: To improve convenience and safety by permitting data transfer as needed concerning an IC card having two completely independent signal processing modules. **SOLUTION:** When it is necessary to transfer data from a contact circuit part 16 to a non-contact circuit part 13, the data of a transfer object axes enciphered by an enciphering part 162 in the contact circuit part 16, signature data ate applied by a signature processing part 163, and these data are stored in a shard memory 19. These data are read out by the non-contact circuit part 13 as them data reception destination, the signature is verified by a signature processing part 133, it is confirmed them data ate surely transferred from the contact circuit part 16, the original data are restored by deciphering data in an enciphering part 132, and these data are stored in a memory 135 and used for ordinary processing in the non-contact circuit part 13 later.



Data supplied from the **esp@cenet** database - Worldwide

(19)日本特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-194799

(P2000-194799A)

(43)公開日 平成12年7月14日 (2000.7.14)

(51)Int.Cl.

G 0 6 K 17/00
19/07

識別番号

F I

C 0 6 K 17/00
19/00

テマコード(参考)

B 5 B 0 3 ü
H 5 B 0 5 8
N

審査請求 未請求 請求項の数15 O L (全 14 頁)

(21)出願番号

特願平10-368157

(22)出願日

平成10年12月24日 (1998.12.24)

(71)出願人

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72)発明者

山田 真生

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

(72)発明者

栗田 直人

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

(74)代理人

100094053

弁理士 佐藤 隆久

Fターム(参考) 5B035 AA00 BB09 CA11 CA25

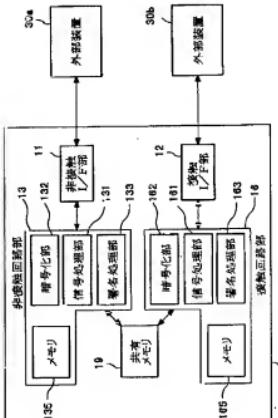
5B058 CA15 KA40

(54)【発明の名称】 携帯型信号処理装置

(57)【要約】

【課題】2つの全く独立した信号処理モジュールを有するICカードにおいて、必要に応じてデータ転送を可能にし、利便性、安全性を高くする。

【解決手段】接触回路部16から非接触回路部13にデータを転送する必要が生じた時には、接触回路部16において、転送対象のデータを暗号化部162で暗号化し、署名処理部163で署名データを付与し、共有メモリ19に記憶する。これを、データ受信先なる非接触回路部13が読み出し、署名処理部133で署名を検証して確かに接触回路部16より転送されてきたデータであることを確認し、暗号化部132において復号化して元のデータを復元し、メモリ135に記憶して、たとえばその後の非接触回路部13における通常の処理において用いる。



【特許請求の範囲】

【請求項1】外部装置と所定の通信方式により通信を行う第1の通信手段と、前記第1の通信手段を介して通信を行い、所望の信号処理を行う第1の信号処理手段と、外部装置と前記第1の通信手段とは異なる所定の通信方式により通信を行う第2の通信手段と、前記第2の通信手段を介して通信を行い、前記第1の信号処理手段とは独立した所望の信号処理を行う第2の信号処理手段と、前記第1の信号処理手段および前記第2の信号処理手段よりアクセス可能な共有領域を有するメモリ手段と、前記第1の信号処理手段および前記第2の信号処理手段の少なくともいずれか一方に設けられ、所望の転送対象のデータを所定の形態に変換し転送用データを生成する転送用データ生成手段と、前記転送用データ生成手段が設けられている前記信号処理手段に設けられ、前記生成された転送用データを、前記メモリ手段の前記共有領域に書き込むデータ書き込み手段と、前記第1の信号処理手段および前記第2の信号処理手段の少なくとも他方に設けられ、前記メモリ手段の前記共有領域に書き込まれた前記転送用データを読み出すデータ読み出し手段と、前記データ読み出し手段が設けられている前記信号処理手段に設けられ、前記転送用データより転送対象の原データを復元する原データ復元手段とを有する携帯型信号処理装置。

【請求項2】外部装置と所定の通信方式により通信を行う第1の通信手段と、前記第1の通信手段を介して通信を行い、所望の信号処理を行う第1の信号処理手段と、外部装置と前記第1の通信手段とは異なる所定の通信方式により通信を行う第2の通信手段と、前記第2の通信手段を介して通信を行い、前記第1の信号処理手段とは独立した所望の信号処理を行う第2の信号処理手段と、前記第1の信号処理手段および前記第2の信号処理手段の少なくともいずれか一方に設けられ、所望の転送対象のデータを所定の形態に変換し転送用データを生成する転送用データ生成手段と、前記転送用データ生成手段が設けられている前記信号処理手段に設けられ、前記生成された転送用データを、対応する前記第1の通信手段または前記第2の通信手段を介して外部に出力するデータ出力手段と、前記第1の信号処理手段および前記第2の信号処理手段の少なくとも他方に設けられ、対応する前記第1の通信手段または前記第2の通信手段を介して外部より入力されるデータであって、前記データ出力手段により出力され前記転送用データが入力されるデータ入力手段と、

前記データ入力手段が設けられている前記信号処理手段に設けられ、前記転送用データより転送対象の原データを復元する原データ復元手段とを有する携帯型信号処理装置。

【請求項3】前記第1の信号処理手段および前記第2の信号処理手段は、各々、所定の暗号化処理に係わる鍵情報を有し、

前記転送用データ生成手段は、前記転送対象のデータを、当該転送用データ生成手段が設けられている前記信号処理手段の前記鍵情報に基づいて暗号化して前記転送用データを生成し、前記原データ復元手段は、前記転送用データを、当該原データ復元手段が設けられている前記信号処理手段の前記鍵情報に基づいて復号化し、前記転送対象の原データを復元する請求項1または2に記載の携帯型信号処理装置。

【請求項4】前記第1の信号処理手段および前記第2の信号処理手段は、各々当該信号処理手段を特定することができる所定のデータを有し、

前記転送用データ生成手段は、前記転送対象のデータに、当該転送用データ生成手段が設けられている前記信号処理手段の前記所定のデータを付加して前記転送用データを生成し、

前記原データ復元手段は、前記転送用データを、当該原データ復元手段が設けられている前記信号処理手段の前記所定のデータに基づいて検証し、適切な前記転送対象の原データを復元する請求項1～3のいずれかに記載の携帯型信号処理装置。

【請求項5】前記信号処理手段を特定することができる所定のデータは署名データである請求項4に記載の携帯型信号処理装置。

【請求項6】前記信号処理手段を特定することができる所定のデータは、メッセージ認証コードである請求項4に記載の携帯型信号処理装置。

【請求項7】外部装置と所定の通信方式により通信を行う第1の通信手段と、所望のデータを記憶する記憶手段を有し、前記第1の通信手段を介した通信に基づいて、当該記憶手段に記憶されているデータを参照して所望の信号処理を行う第1の信号処理手段と、

外部装置と前記第1の通信手段とは異なる所定の通信方式により通信を行う第2の通信手段と、所望のデータを記憶する記憶手段を有し、前記第2の通信手段を介した通信に基づいて、当該記憶手段に記憶されているデータを参照して、前記第1の信号処理手段とは独立した所望の信号処理を行う第2の信号処理手段と、

前記第2の信号処理手段の前記記憶手段に記憶されているデータを前記第1の信号処理手段に転送するデータ転送手段と前記第1の信号処理手段に設けられ、必要に応

じて、前記第1の通信手段を介して通信を行う外部装置が、前記第2の信号処理手段が前記第2の通信手段を介して通信を行い所定の処理を行う外部装置として適切か否かの認証処理を行う認証手段とを有し、前記第1の信号処理手段は、前記認証処理の結果、前記第1の通信手段を介して通信を行う外部装置が、前記第2の信号処理手段が前記第2の通信手段を介して通信を行い所定の処理を行う外部装置として適切であった場合に、前記転送される前記第2の信号処理手段の前記記憶手段に記憶されていたデータに基づいて、前記第1の通信手段を介して通信を行う前記外部装置と通信を行い、前記所定の処理を行う携帯型信号処理装置。

【請求項8】前記第1の信号処理手段は、前記認証処理の結果、前記第1の通信手段を介して通信を行う外部装置が、前記第2の信号処理手段が前記第2の通信手段を介して通信を行い所定の処理を行う外部装置として適切であった場合に、前記転送される前記第2の信号処理手段の前記記憶手段に記憶されていたデータを、前記第1の通信手段を介して通信を行う前記外部装置に送出する請求項7に記載の携帯型信号処理装置。

【請求項9】外部装置と所定の通信方式により通信を行う第1の通信手段と、前記第1の通信手段を介して通信を行い、所望の信号処理を行う第1の信号処理手段と、外部装置と前記第1の通信手段とは異なる所定の通信方式により通信を行う第2の通信手段と、

前記第2の通信手段を介して通信を行い、前記第1の信号処理手段とは独立した所望の信号処理を行う第2の信号処理手段と、前記第1の信号処理手段および前記第2の信号処理手段によりアクセス可能な共有領域を有するメモリ手段と、少なくとも前記第2の信号処理手段に設けられ、所望の転送対象のデータを所定の形態に変換し転送用データを生成する転送用データ生成手段と、前記転送用データ生成手段に設けられ、前記生成された転送用データを、前記メモリ手段の前記共有領域に書き込むデータ書き込み手段と、

少なくとも前記第1の信号処理手段に設けられ、前記メモリ手段の前記共有領域に書き込まれた前記転送用データを読み出すデータ読み出し手段と、前記データ読み出し手段が設けられている前記信号処理手段に設けられ、前記生成された転送用データを、前記メモリ手段の前記共有領域に書き込むデータ書き込み手段と、

【請求項10】外部装置と所定の通信方式により通信を行う第1の通信手段と、前記第1の通信手段を介して通信を行い、所望の信号処理を行う第1の信号処理手段と、

外部装置と前記第1の通信手段とは異なる所定の通信方式により通信を行う第2の通信手段と、

前記第2の通信手段を介して通信を行い、前記第1の信号処理手段とは独立した所望の信号処理を行う第2の信号処理手段と、

前記第1の信号処理手段および前記第2の信号処理手段によりアクセス可能な共有領域を有するメモリ手段と、少なくとも前記第1の信号処理手段に設けられ、対応する前記第1の通信手段を介して前記第2の信号処理手段に対して外部より入力されるデータであって、所望の転送対象のデータが所定の形態に変換された転送用データが入力されるデータ入力手段と、

前記データ入力手段が設けられている前記信号処理手段に設けられ、前記入力された転送用データを、前記メモリ手段の前記共有領域に書き込むデータ書き込み手段と、

少なくとも前記第2の信号処理手段に設けられ、前記メモリ手段の前記共有領域に書き込まれた前記転送用データを読み出すデータ読み出し手段と、

前記データ読み出し手段が設けられている前記信号処理手段に設けられ、前記読み出された前記転送用データより転送対象の原データを復元する原データ復元手段とを有する携帯型信号処理装置。

【請求項11】前記転送用データは、所定の暗号化処理により転送対象の原データを暗号化したデータであり、少なくとも前記第2の信号処理手段は、前記所定の暗号化処理を解読する鍵情報を有し、

前記原データ復元手段は、前記転送用データを、前記第2の信号処理手段の前記鍵情報に基づいて復元し、前記転送対象の原データを復元する請求項10に記載の携帯型信号処理装置。

【請求項12】前記転送用データは、転送先の前記信号処理手段を特定することのできる所定のデータが付加されたデータであり、

前記原データ復元手段は、前記転送用データを、前記所定のデータに基づいて検証し、適切な前記転送対象の原データを復元する請求項10または11に記載の携帯型信号処理装置。

【請求項13】前記信号処理手段を特定することのできる所定のデータは署名データである請求項12に記載の携帯型信号処理装置。

【請求項14】前記信号処理手段を特定することのできる所定のデータは、メッセージ認証コードである請求項12に記載の携帯型信号処理装置。

【請求項15】前記第1の通信手段または前記第2の通信手段のいずれか一方は、無線通信により非接触式で外部装置と通信を行う非接触式通信手段であり、

前記第1の通信手段または前記第2の通信手段のいずれか他方は、電極を介して接触式で前記外部装置と通信を行う接触式通信手段である請求項1～14のいずれかに

記載の携帯型信号処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、たとえば接触方式および非接触方式というような複数の通信手段、および、その通信手段に応じた複数の信号処理手段を有する、たとえばカード形状の携帯型信号処理装置であって、それら複数の信号処理手段および外部装置との間ににおいて、データの転送をセキュリティ性を十分確保した上で適切に行うことができる携帯型信号処理装置に関するもの。

【0002】

【従来の技術】半導体技術や実装技術の進展により、カード内にメモリや演算処理回路を具えたいわゆるICカードの開発、利用が急速に進んでいる。このようなICカードには、大きく分けて、カード表面に設けられた電極を介して外部のリード／ライト装置とICカードとで信号を送受する接触型のICカードと、アンテナコイルを介した電磁波などにより信号を送受する非接触型のICカードがある。接触型ICカードは、電力の供給が安定しているため複雑な演算処理を高速に行うことが可能となり、セキュリティ性の高い用途に適用することができる。一方、非接触型ICカードは、取り扱いが容易であるためゲートの通過許諾用など比較的処理の簡単な用途には適しているが、一般的に電力供給が不安定なため、複雑な演算処理を高速に行わせるのは難しい。

【0003】また最近では、カードの多機能化への要望などがあり、1枚のカードに接触型ICカードと非接触型ICカードの両方の機能を持ったカードも使用され始めている。1枚のカードに接触型ICカードと非接触型ICカードの両方の機能を持つ方式としては、信号処理部も含めて全く別の構成の接触型ICカードICモジュールとアンテナ付非接触型の両方式で動作するICチップを用いる信号処理装置を共有しない方式と、信号処理装置を共有しインクース部のみ分かれている方式とがある。これらのいずれの方式においても、外部のリード／ライト装置との通信は、接触型ICカードとしてはカード表面の所定の位置に設けられた電極を介して行われ、非接触型ICカードとしてはカード内に内蔵されるアンテナコイルを介して行われる。なお、これらのカードの構成を機能的に外部から捉えた場合は、図10～図12のように表すことができる。

【0004】

【発明が解決しようとする課題】ところで、このような接触型ICカードと非接触型ICカードの両方の機能を有するICカードにおいて、それら両方の方式の処理により同一のデータを取り扱うようにすると、そのセキュリティレベルは、実質的に非接触型の低いレベルとなってしまい、接触型ICカードとしての高セキュリティ性を維持することができないという不利益がある。そのため、特に信号処理回路や記憶回路を各々含む接触型および非接触型の各モジュールを別個に有するようないCカードにおいては、それら接触型モジュールおよび非接触型モジュールを完全に切り分け、これら各モジュールの特徴を維持するようしている場合が多い。しかし、そのような構成においては、同一のカード基板中に収容されている2つのモジュールの間において、全くデータの転送などを行うことができず、これら2つのモジュールを使使してより利便性の高い使用形態とすることや、2つのモジュールを補完させてより安全性の高い形態で使用することなどができないという問題が生じる。

【0005】したがって、本発明の目的は、少なくとも通信手段の異なる2つの信号処理モジュールを有するICカードなどの携帯型信号処理装置において、必要に応じて信号処理モジュール間でデータ転送が可能で、利便性、安全性ともにより高い携帯型信号処理装置を提供することにある。

【0006】

【課題を解決するための手段】前記課題を解決するため、本発明の携帯型信号処理装置は、外部装置と所定の通信方式により通信を行う第1の通信手段と、第1の通信手段を介して通信を行い、所望の信号処理を行う第1の信号処理手段と、外部装置と第1の通信手段とは異なる所定の通信方式により通信を行う第2の通信手段と、第2の通信手段を介して通信を行い、第1の信号処理手段とは独立した所望の信号処理を行う第2の信号処理手段と、第1および第2の信号処理手段によりアクセス可能な共有領域を有するメモリ手段と、第1および第2の信号処理手段の少なくともいずれか一方に設けられ、所望の転送対象のデータを所定の形態に変換し転送用データを生成する転送用データ生成手段と、転送用データ生成手段が設けられている信号処理手段に設けられ、生成された転送用データを、メモリ手段の共有領域に書き込むデータ書き込み手段と、第1および第2の信号処理手段の少なくとも他方に設けられ、メモリ手段の共有領域に書き込まれた転送用データを読み出すデータ読み出し手段と、データ読み出し手段が設けられている信号処理手段に設けられ、転送用データより転送対象の原データを復元する原データ復元手段とを有する。

【0007】また、本発明の携帯型信号処理装置は、外部装置と所定の通信方式により通信を行う第1の通信手段と、第1の通信手段を介して通信を行い、所望の信号処理を行う第1の信号処理手段と、第1の通信手段とは異なる所定の通信方式により通信を行う第2の通信手段と、第2の通信手段を介して通信を行い、第1の信号処理手段とは独立した所望の信号処理を行う第2の信号処理手段と、第1および第2の信号処理手段の少なくともいずれか一方に設けられ、所望の転送対象のデータを所定の形態に変換し転送用データを生成する転送用データ生成手段と、転送用データ生成手段が設けら

れている信号処理手段に設けられ、生成された転送用データを、対応する第1または第2の通信手段を介して外部に出力するデータ出力手段と、第1および第2の信号処理手段の少なくとも一方に設けられ、対応する第1または第2の通信手段を介して外部より入力されるデータであって、データ出力手段より出力された転送用データが入力されるデータ入力手段と、データ入力手段が設けられている信号処理手段に設けられ、転送用データより転送対象の原データを復元する原データ復元手段とを有する。

【0008】また、本発明の携帯型信号処理装置は、外部装置と所定の通信方式により通信を行う第1の通信手段と、所望のデータを記憶する記憶手段を有し、第1の通信手段を介した通信に基づいて、当該記憶手段に記憶されているデータを参照して所望の信号処理を行う第1の信号処理手段と、外部装置と第1の通信手段とは異なる所定の通信方式により通信を行う第2の通信手段と、所望のデータを記憶する記憶手段を有し、第2の通信手段を介した通信に基づいて、当該記憶手段に記憶されているデータを参照して、第1の信号処理手段とは独立して所望の信号処理を行う第2の信号処理手段と、第2の信号処理手段の記憶手段に記憶されているデータを第1の信号処理手段に転送するデータ転送手段と、第1の信号処理手段に設けられ、必要に応じて、第1の通信手段を介して通信を行う外部装置が、第2の信号処理手段が第2の通信手段を介して通信を行所定の処理を行う外部装置として適切か否かの認証処理を行う認証手段とを有し、第1の信号処理手段は、認証処理の結果、第1の通信手段を介して通信を行外部装置が、第2の信号処理手段が第2の通信手段を介して通信を行所定の処理を行う外部装置として適切であった場合に、前記転送される第2の信号処理手段の記憶手段に記憶されていたデータに基づいて、第1の通信手段を介して通信を行外部装置と通信を行い、所定の処理を行う。

【0009】また、本発明の携帯型信号処理装置は、外部装置と所定の通信方式により通信を行う第1の通信手段と、第1の通信手段を介して通信を行い、所望の信号処理を行う第1の信号処理手段と、外部装置と第1の通信手段とは異なる所定の通信方式により通信を行う第2の通信手段と、第2の通信手段を介して通信を行い、第1の信号処理手段とは独立した所望の信号処理を行う第2の信号処理手段と、第1および第2の信号処理手段よりアクセス可能な共有領域を有するメモリ手段と、少なくとも第2の信号処理手段に設けられ、所望の転送対象のデータを所定の形態に変換し転送用データを生成する転送用データ生成手段と、転送用データ生成手段が設けられている信号処理手段に設けられ、生成された転送用データを、メモリ手段の共有領域に書き込むデータ書き込み手段と、少なくとも第1の信号処理手段に設けられ、メモリ手段の共有領域に書き込まれた転送用データを読み出すデータ読み出し手段と、データ読み出し手段が設けられている信号処理手段に設けられ、読み出された転送用データより転送対象の原データを復元する原データ復元手段とを有する。

【0010】さらに、本発明の携帯型信号処理装置は、外部装置と所定の通信方式により通信を行う第1の通信手段と、第1の通信手段を介して通信を行、所望の信号処理を行う第1の信号処理手段と、外部装置と第1の通信手段とは異なる所定の通信方式により通信を行第2の通信手段と、第2の通信手段を介して通信を行、第1の信号処理手段とは独立した所望の信号処理を行う第2の信号処理手段と、第1および第2の信号処理手段よりアクセス可能な共有領域を有するメモリ手段と、少なくとも第1の信号処理手段に設けられ、対応する第1の通信手段を介して第2の信号処理手段に対して外部より入力されるデータであって、所望の転送対象のデータが所定の形態に変換された転送用データが入力されるデータ入力手段と、データ入力手段が設けられている信号処理手段に設けられ、入力された転送用データを、メモリ手段の共有領域に書き込むデータ書き込み手段と、少なくとも第2の信号処理手段に設けられ、メモリ手段の共有領域に書き込まれた転送用データを読み出すデータ読み出し手段と、データ読み出し手段が設けられている信号処理手段に設けられ、読み出された転送用データより転送対象の原データを復元する原データ復元手段とを有する。

【0011】

【発明の実施の形態】第1の実施の形態

本発明の携帯型信号処理装置の第1の実施の形態について、図1および図2を参照して説明する。図1は、第1の実施の形態のICカード1の構成を示すブロック図である。ICカード1は、非接触インターフェース(I/F)部11、接触インターフェース(I/F)部12、非接触回路部13、接触回路部16および共有メモリ19を有する。また、非接触回路部13は、信号処理部113、暗号化部132、署名処理部133およびメモリ135を有し、接触回路部16は、信号処理部161、暗号化部162、署名処理部163およびメモリ165を有する。

【0012】まず、ICカード1の各部の構成について図1を参照して説明する。非接触I/F部11は、ICカード1を非接触型カードとして使用する場合の非接触回路部13と外部リード/ライト装置30とのインターフェース回路であり、アンテナコイル、アンテナコイルを介して外部装置より供給される電力を抽出するための整流回路、定電圧回路、アンテナコイルの出力信号より外部装置から送信されたデータを抽出するための検波回路、増幅回路、および、アンテナコイルを介して外部装置にデータを送信するための変調回路などを有する。

【0013】接触I/F部12は、ICカード1を接触

型カードとして使用する場合の接触回路部16と外部リード／ライト装置30bとのインターフェース回路であり、ICカード1と外部リード／ライト装置30bとを電気的に接続するための電極などを有する。本実施の形態においてその電極は、接触型ICカードの規格に基づいた所定の位置に8個設けられており、各々回路電源供給端子、信号用電源供給端子、接地端子、クロック入力端子、リセット端子、データ出入力用端子、およびリザーブ用端子(2個)として定義化されている。

【0014】非接触回路部13の信号処理部131は、メモリ135に予め記憶されている処理プログラムに従って、非接触I/F部11を介して外部リード／ライト装置30aと適宜通信を行いながら、所望の信号処理を行う。この際、信号処理部131は、メモリ135に設定されているパラメータ、データなどを参照し、また、信号処理の結果得られたデータなどを必要に応じて適宜メモリ135に記憶しながら、所望の信号処理を行う。また、信号処理部131は、接触回路部16に対してデータの送信を行う場合には、暗号化部132を制御して送信対象のデータを暗号化し、署名処理部133を制御して署名データを付加して、共有メモリ19に格納する。また、接触回路部16よりデータを受信する必要がある場合には、共有メモリ19よりその転送データを読み出し、署名処理部133を制御して署名データを検証して確かに接触回路部16より転送されたデータであることを確認し、暗号化部132を制御して復号化を行い元の転送対象のデータを得る。

【0015】非接触回路部13の暗号化部132は、信号処理部131からの制御に基づいて、所望のデータに対して、メモリ135に記憶されている所定の暗号鍵を用いて所定の方式により暗号化処理を行う。また、所望の暗号化されたデータに対して、同じくメモリ135に記憶されている暗号鍵を用いて所定の方式により復号化処理を行い、元のデータを復元する。

【0016】非接触回路部13の署名処理部133は、信号処理部131からの制御に基づいて、所望のデータに対してメモリ135に記憶されている署名データを付加する。また、所望の署名データを有するデータに対して、その署名データを検証し、そのデータが適切なデータか否かをチェックする。

【0017】非接触回路部13のメモリ135は、前述したような、信号処理部131で実行するプログラム、パラメータなどのデータや、暗号化部132で用いる暗号鍵データ、署名処理部133で用いる署名データ、あるいは、信号処理部131で実行される処理にともなう入力データ、一時的な処理データ、最終結果データなどが記憶される不揮発性メモリである。

【0018】接触回路部16の信号処理部161は、メモリ165に予め記憶されている処理プログラムに従つて、

接触I/F部12を介して外部リード／ライト装置30bと適宜通信を行いながら、所望の信号処理を行う。この際、信号処理部161は、メモリ165に設定されているパラメータ、データなどを参照し、また、信号処理の結果得られたデータなどを必要に応じて適宜メモリ165に記憶しながら、所望の信号処理を行う。また、信号処理部161は、非接触回路部13に対してデータの送信を行う必要がある場合には、暗号化部162を制御して転送対象のデータを暗号化し、署名処理部163を制御して署名データを付加して、共有メモリ19に格納する。また、所望の信号処理部163を制御して署名データを検証して確かに非接触回路部13より転送されたデータであることを確認し、暗号化部162を制御して復号化を行い元の転送対象のデータを得る。

【0019】接触回路部16の暗号化部162は、信号処理部161からの制御に基づいて、所望のデータに対して、メモリ165に記憶されている所定の暗号鍵を用いて所定の方式により暗号化処理を行う。また、所望の暗号化されたデータに対して、同じくメモリ165に記憶されている暗号鍵を用いて所定の方式により復号化処理を行い、元のデータを復元する。

【0020】接触回路部16の署名処理部163は、信号処理部161からの制御に基づいて、所望のデータに対してメモリ165に記憶されている署名データを付加する。また、所望の署名データを有するデータに対して、その署名データを検証し、そのデータが適切なデータか否かをチェックする。

【0021】接触回路部16のメモリ165は、前述したような、信号処理部161で実行するプログラム、パラメータなどのデータや、暗号化部162で用いる暗号鍵データ、署名処理部163で用いる署名データ、あるいは、信号処理部161で実行される処理にともなう入力データ、一時的な処理データ、最終結果データなどが記憶される不揮発性メモリである。

【0022】共有メモリ19は、非接触回路部13および接触回路部16の両方からアクセス可能なメモリであり、非接触回路部13と接触回路部16との間で転送されるデータが一時的に記憶される不揮発性メモリである。

【0023】次に、このような構成のICカード1の動作について図2を参照して説明する。図2は、図1に示したICカード1の非接触回路部13と接触回路部16の間で直接的にデータ転送を行う場合の動作を模式的に示した図である。まず、通常にICカード1を使用する時であって、ICカード1を非接触型ICカードとして使用する時には、使用者はICカード1をたえとえ外部リード／ライト装置30aにかざさなどして近づける。

すると、ICカード1においては、非接触I/F部1のアンテナコイルを介して電力が供給され、非接触回路部13が起動される。そして、信号処理部131がメモリ135に記憶されているプログラムに従って処理を開始し、適宜外部リード/ライト装置30aと通信を行なうながら所望の処理を行う。

【0024】また、通常にICカード1を使用する時であって、ICカード1を接触型ICカードとして使用する時には、使用者はICカード1をたとえば外部リード/ライト装置30bに挿入するなどする。すると、ICカード1には接触I/F部12の電源供給端子を介して電力が供給され、接触回路部16が起動される。そして、信号処理部161が、メモリ165に記憶されているプログラムに従って処理を開始し、適宜外部リード/ライト装置30bと通信を行なうながら所望の処理を行う。

【0025】そして、このような非接触型ICカードおよび接触型ICカードとしての通常の処理の中で、あるいは、外部リード/ライト装置30a、30bなどからの特殊な指示などにより、接触回路部16と非接触回路部13との間でデータを転送する必要生じた時には、図2に示すように、たとえばデータ送信元である接触回路部16において、転送対象のデータを暗号化部162で暗号化し、署名処理部163で署名データを付与し、共にメモリ19に記憶する。これを、データ受信元たる非接触回路部13が読み出し、署名処理部133で署名を検証して確かに接触回路部16より転送されてきたデータであることを確認し、暗号化部132において復号化して元のデータを復元し、メモリ135に記憶して、たとえばその後の非接触回路部13における通常の処理において用いる。なお、データの転送が非接触回路部13から接触回路部16に対して行われる場合も、これと同様の処理により行われる。

【0026】このように、ICカード1においては、共有メモリ19を用いることにより、実質的にICカード内においてその構成が全く分離されている非接触回路部13と接触回路部16との間で、データの転送を行うことができる。そして、そのデータの転送は、転送データを暗号化したり署名データを付加するなどしているので、安全に行なうことができる。したがって、非接触回路部13と接触回路部16とが分離された構成のセキュリティ性が高いICカードに対して、その安全性を維持した状態で、より利便性の高い使用形態を提供することができる。

【0027】なお、第1の実施の形態においては、転送データに、メッセージ認証コード(MAC: Message Authentication Code)を付加し、転送データの完全性を確実に検証・維持できるようにもよい。その際に、たとえば署名データが付加されたデータに対してさらにメッセージ認証コード(MAC)を付加してもよい

し、署名データの付加は行わずに、暗号化されたデータに対してメッセージ認証コード(MAC)を付加してもよい。これら、暗号化、署名データの付加およびメッセージ認証コード(MAC)の付加の各処理は、任意の組み合せで選択的に行ってよい。

【0028】第2の実施の形態

本発明の携帯型信号処理装置の第2の実施の形態について、図3および図4を参照して説明する。図3は、第2の実施の形態のICカード2の構成を示すブロック図である。ICカード2は、非接触インターフェース(1/F)部11、接触インターフェース(I/F)部12、非接触回路部13および接触回路部16を有する。また、非接触回路部13は、信号処理部131、暗号化部132、署名処理部133およびメモリ135を有し、接触回路部16は、信号処理部161、暗号化部162、署名処理部163およびメモリ165を有する。

【0029】ICカード2の構成は、図3よりも明らかなように、第1の実施の形態のICカード1において共有メモリ19が設けられていない構成である。ICカード2のその他の構成部については、その機能も含めて第1の実施の形態のICカード1の対応する各構成部が同一である。なお、そのため、各構成部の説明は省略する。第1の実施の形態のICカード1においては、共有メモリ19を介して非接触回路部13と接触回路部16がICカード1内でデータの転送を行うことができたが、第2の実施の形態のICカード2においては、非接触回路部13と接触回路部16が全く独立な構成となっており、内部でデータの転送を行うことができない。換言すれば、各回路部の独立性はICカード1より高く、たとえば接触回路部16で扱うセキュリティ性の高いデータなどはより安全にコントロールされていることになる。

【0030】図4は、図3に示したICカード2の非接触回路部13と接触回路部16の間でデータ転送を行う場合の動作を模式的に示した図である。ICカード2における、通常使用時の動作も、第1の実施の形態のICカード1と同じなので、説明は省略する。このような構成のICカード2においても、非接触回路部13または接触回路部16で処理しているデータなどを、他方の回路部で参照したい場合や使用したい場合などが生じ得る。その際のICカード2の動作について図4を参照して説明する。

【0031】ICカード2において、接触回路部16と非接触回路部13との間でデータを転送する必要が生じた時には、図4に示すように、たとえばデータ送信元たる接触回路部16において、転送対象のデータを暗号化部162で暗号化し、署名処理部163で署名データを付与し、接触I/F部12を介して、外部リード/ライト装置30に出力する。この際、出力したデータがICカード2の非接触I/F部11に入力されるように、必要に応じて、たとえばデータ転送先を外部リード/ラ

イト装置30に対して指示するなどの制御を行う。

【0032】そのようなデータ転送先の制御により、あるいは、子め非接触回路部13または接触回路部16との通信により動作が設定されていた外部リード／ライト装置30における処理により、接触回路部16より出力されたデータが非接触I／F部11に入力されると、非接触I／F部11はそのデータを非接触回路部13に入力する。非接触回路部13は、通常の非接触回路部13としての処理の中で、入力されたデータに対して署名処理部133で署名を検証して接触回路部16より転送されてきたデータであることを検出し、暗号化部132において復号化して元のデータを復元し、メモリ135に記憶するなどして、たとえばその後の処理に用いる。なお、データの転送が非接触回路部13から接触回路部16に対して行われる場合も、これと同様の処理により行われる。

【0033】このように、たとえば共有メモリを有しておらず、非接触回路部13と接触回路部16が直接的にデータの転送が行えないよう構成したICカード2においても、適切に所望のデータの転送を行なうことができる。そして、そのデータの転送は、外部装置を介して行うことになるが、転送データを暗号化し署名データを附加するなどしているので、安全に行なうことができる。したがって、非接触回路部13と接触回路部16とが完全に分離された構成の非常にセキュリティ性が高いICカードに対しても、その安全性を維持した状態で、より利便性の高い使用形態を提供することができる。

【0034】なお、図3において、外部リード／ライト装置30は1つの装置として示したが、たとえばICカード2の非接触型および接触型の各インターフェースに応じた別個の装置であってもよい。また、ICカード2からのデータの送出およびそのデータのICカード2への転送は、異なる時間帯に行われるものであってもよい。また、第1の実施の形態と同様に、転送データに、メッセージ認証コード(MAC)を付加し、転送データの完全性を確実に検証・維持するようにしてもよい。

【0035】第3の実施の形態

本発明の携帯型信号処理装置の第3の実施の形態について、図5および図6を参照して説明する。図5は、第3の実施の形態のICカード3の構成を示すブロック図である。ICカード3は、非接触インターフェース(I/F)部11、接触インターフェース(I/F)部12、非接触回路部13、接触回路部16およびデータ転送部20を有する。また、非接触回路部13は、信号処理部131、認証処理部134およびメモリ135を有し、接触回路部16は、信号処理部161、認証処理部164およびメモリ165を有する。

【0036】まず、ICカード3の構成について図5を参照して説明する。なお、ICカード3の構成も、基本的にには、前述した第1および第2の実施の形態のICカ

ード1、2と同様の構成である。したがって、機能が同一の構成部については、同一の符号を付して、その説明を省略する。非接触回路部13の認証処理部134は、非接触I／F部11を介して接続される外部リード／ライト装置30aが、非接触回路部13と接続を行いデータの送受を行なう対象として適切な装置か否かを検査するための認証処理を行なう。接觸回路部16の認証処理部164も、認証処理部134と同様に、接觸I／F部12を介して接続される外部リード／ライト装置30bが、接觸回路部16と接続を行いデータの送受を行なう対象として適切な装置か否かを検査するための認証処理を行なう。これら認証処理部134および認証処理部164における認証処理は、具体的には、たとえば前述したような暗号を用いた処理や、署名を用いた処理、あるいはPIN照合などである。

【0037】データ転送部20は、非接触回路部13と接觸回路部16との間のデータの転送を行なう。データ転送部20は、非接触回路部13の信号処理部131または接觸回路部16の信号処理部161により制御され、非接触回路部13と接觸回路部16の間で所望のデータの転送を行なう。データ転送部20は、たとえば不揮発性メモリで構成されたバッファを有するような構成であり、非接触回路部13および接觸回路部16が同時に有効とならなくても、適切にデータの転送が行えるようになっている。

【0038】次に、ICカード3の動作について図6を参照して説明する。図6は、図5に示したICカード3の非接触回路部13と接觸回路部16の間で直接的にデータ転送を行なう場合の動作を模式的に示した図である。ICカード3における、通常使用時の動作は、第1および第2の実施の形態のICカード1、2と同じなので、説明は省略する。ここでは、たとえば、接觸I／F部12の不良などにより、接觸回路部16と外部リード／ライト装置30bが通信を行えなくなったような場合のICカード3の動作について説明する。

【0039】接觸I／F部12が不良になった場合、そのままでは接觸回路部16に蓄積されているデータなどが使用できなくなるため、それらのデータを外部の処理装置に伝送する必要がある。そのために、使用者は、接觸回路部16と通信を行って所望の処理を行なう外部装置30bと実質的に接続されている非接触インターフェースを有する外部リード／ライト装置30aに対して、ICカード3をかざすなどして、実質的にICカード3と外部リード／ライト装置30aを接続する。これにより、ICカード3においては、非接触I／F部11のアンテナコイルを介して電力を供給され、非接触回路部13が起動され、信号処理部131がメモリ135に記憶されているプログラムに従って処理を開始する。

【0040】そしてまず、信号処理部131からの指示に基づいて、図6に示すように、認証処理部134が非

接触I/F部11を介して外部リード/ライト装置30aと通信を行い、外部リード/ライト装置30aが、接触I/F部12を介して接触回路部16と通信を行って所望の処理を行う外部装置bか否か、あるいは、その外部装置30bに接続された装置か否か、外部リード/ライト装置30aの認証処理を行う。その結果、外部リード/ライト装置30aが正当な装置であると判定された場合には、非接触回路部13の信号処理部131は、データ転送部20および接触回路部16の信号処理部161を介して、接触回路部16のメモリ16より所望のデータを読み出し、非接触I/F部11を介して外部リード/ライト装置30aに出力する。なお、非接触I/F部11が不良で、非接触回路部13より接触回路部16に対してデータの転送が行われる場合も、これと同様の処理により行われる。

【0041】このように、ICカード3においては、非接触回路部13と接触回路部16が別個の構成となっている場合においても、たとえば、いずれかの回路や出入力I/Fに不良が発生したような場合には、一方のデータを他方の回路に転送し、その後の塑型に使用することができる。したがって、2つの回路間の独立性を維持して各データのセキュリティ性などを維持した状態で、それら各データを取り扱う上の安全性および利便性を高めることができる。

【0042】なお、第1および第2の実施の形態と同様に、転送データを暗号化したり、転送データに署名データやメッセージ認証コード(MAC)を付加し、転送データの完全性を確実に検証・維持できるようにしてもよい。

【0043】第4の実施の形態

本発明の携帯型信号処理装置の第4の実施の形態について、図7～図9を参照して説明する。図7は、第4の実施の形態のICカード4の構成を示すブロック図である。ICカード4は、非接触インターフェース(I/F)部11、接触インターフェース(I/F)部12、非接触回路部13、接触回路部16および共有メモリ19を有する。また、非接触回路部13は、信号処理部131およびメモリ135を有し、接触回路部16は、信号処理部161、署名処理部163およびメモリ16よりメモリ16を有する。

【0044】ICカード4の構成は、図7よりも明らかのように、第1の実施の形態のICカード1の構成に含まれるものである。したがって、ICカード4の各構成部には対応するICカード1の各構成部と同一の符号を付して、その説明を省略する。そして、ICカード4とICカード1との違いは、非接触回路部13の内部構成として暗号化部132および署名処理部133を必須としない点、接触回路部16の内部構成として暗号化部162を必須としない点、および、接触回路部16の署名処理部163の処理内容が異なる点である。ICカード4の

接触回路部16の署名処理部163bは、たとえばRSA署名など、複雑で膨大な計算量が必要な署名処理を行う。このような演算処理は、使用電力が不安定で制限のある非接触回路部13においては実現できない機能である。

【0045】このような構成のICカード4の動作について、図8および図9を参照して説明する。図8は、図7に示したICカード4の動作を模式的に示す第1の図であり、図9は、図7に示したICカード4の動作を模式的に示す第2の図である。ICカード4の通常の動作は、前述した各実施の形態と同じであるので、ここでは、高度な署名検証処理を行わなければならず通常の非接触ICカードでは実行できない処理と、ICカード4において非接触インターフェースにより実行する場合の動作について説明する。

【0046】まず、外部装置からデータを転送される時ののようなICカード4の動作について図8を参照して説明する。たとえば、ICカード4と外部リード/ライト装置30aとの非接触I/F部11を介した通常の処理の結果、外部リード/ライト装置30aからICカード4に対して、ICカード4の使用者の課金情報など、セキュリティ性が高いためRSA署名が付されたデータが転送されたとする。この場合、ICカード4は、この情報を共有メモリ19を介して非接触回路部13から接触回路部16に転送する。この共有メモリ19に介した転送方法については、第1の実施の形態のICカード1と同じである。そして、そのようなデータを受け取った接触回路部16は、署名処理部163bによりそのRSA署名を用いた検証を行い、そのデータの正当性を確認し、そのデータをメモリ16より書き込むなどして、以後の処理を行う。

【0047】この処理について具体的に例示して説明する。たとえば、ICカード4の使用者が、ICカード4を非接触型ICカードとして用いて、所定金額の支払い処理を行ったとする。この処理は、ICカード4の非接触回路部13と外部リード/ライト装置30aとの間で通常に行われるが、その結果、その課金処理を示すデータが、RSA署名処理が行われて、最終的に非接触回路部13に入力される。非接触回路部13においては、入力されたデータは、直ちに共有メモリ19に記録しておこう。

【0048】このような個別の支払い処理は、直ちに行われ、その都度、その課金データが順次共有メモリ19に蓄積される。そして、何らかのきっかけによりICカード4の接触回路部16が有効にされた際に、接触回路部16は共有メモリ19よりその課金データを読み出し、署名処理部163bによりそのデータの正当性をチェックし、正當であれば、実質的に決裁を行う処理を行う。これにより、ICカード4内で、決裁処理を高いセキュリティ性で行うことができる。

【0049】次に、外部装置へデータを転送する時のI Cカード4の動作について図9を参照して説明する。たとえば、非接触回路部13で、署名処理を行って高いセキュリティ性で送信したいデータが発生した場合には、非接触回路部13はそのデータを、共有メモリ19を介して接触回路部16に転送しておく。接触回路部16においては、そのデータに対して、署名処理部163bにおいてR.S.A署名を行う処理を行い、署名を行った転送用データを共有メモリ19を介して、再び非接触回路部13に転送する。非接触回路部13は、この署名されたデータを非接触I/F部11を介して外部リード/ライト装置30aに出力する。その結果、外部リード/ライト装置30aにおいては、このデータに対して認証処理を行い、適切なデータと判定された場合には所望の情報処理に用いる。

【0050】このように、I Cカード4においては、非接触型I Cカードとして使用する場合に、R.S.A署名を行ったデータを用いることができ、取り扱うデータの信頼性、セキュリティ性を高めることができる。

【0051】変形例

なお、本発明は前述した各実施の形態に限られるものではなく、任意好適な種々の変更が可能である。たとえば、前述した各実施の形態においては、データの伝送の流れおよびそれに伴うデータに対する認証処理についてのみ説明したが、これらのデータの種類、また、実際にデータが転送されるための処理、操作などは、任意である。また、本発明は、複数の通信手段を有することを要件としているが、これは、本実施の形態のように接触式および非接触式について各々少なくとも1つ有することを必要とするものではない。全て接触式あるいは非接触式の方式であって、プロトコルなどが異なる複数の通信手段を有する携帯型信号処理装置であっても、複数の通信手段を有する携帯型信号処理装置であることは明らかであり、本発明の範囲内である。

【0052】また、本実施の形態においては、カード形状の装置であるいわゆるI Cカードを例示して本発明を説明したが、本発明はこれに限られるものではない。たとえば種々の形状で実現されているいわゆるタグ形態で実施してもよいし、手帳程度の大きさの機器として実施するようにしてもよい。また、本発明の携帯型信号処理装置の適用範囲は何ら限定されるものではない。電子マネーやプリペイドカードのような用途や、定期券のようなゲート通過のための装置を始めとする、任意の対象に對して適用してよい。

【0053】また、前述した各携帯型信号処理装置において、非接触回路部13と接触回路部16は、物理的に別々のチップに構成されたものであっても、1つのチップに構成されたものであってもよく、その構成は何ら限界はない。その他、携帯型信号処理装置のハードウェア構成や、通信プロトコルの種類なども任

意の構成、任意のプロトコルでよい。

【0054】

【発明の効果】以上説明したように、本発明によれば、少なくとも通信手段の異なる2つの信号処理モジュールを有する携帯型信号処理装置であって、必要に応じて信号処理モジュール間でデータ転送が可能で、利便性、安全性ともにより高い携帯型信号処理装置を提供することができる。

【図面の簡単な説明】

【図1】図1は、本発明の第1の実施の形態のI Cカードの構成を示すブロック図である。

【図2】図2は、図1に示したI Cカードの非接触回路部と接触回路部の間で直接的にデータ転送を行う場合の動作を模式的に示す図である。

【図3】図3は、本発明の第2の実施の形態のI Cカードの構成を示すブロック図である。

【図4】図4は、図3に示したI Cカードの非接触回路部と接触回路部の間でデータ転送を行う場合の動作を模式的に示す図である。

【図5】図5は、本発明の第3の実施の形態のI Cカードの構成を示すブロック図である。

【図6】図6は、図5に示したI Cカードの動作を模式的に示す図である。

【図7】図7は、本発明の第4の実施の形態のI Cカードの構成を示すブロック図である。

【図8】図8は、図7に示したI Cカードの動作を模式的に示す第1の図である。

【図9】図9は、図7に示したI Cカードの動作を模式的に示す第2の図である。

【図10】図10は、接触型I Cカードと非接触型I Cカードの両方の機能を有するI Cカードの構成の例を示す第1の図である。

【図11】図11は、接触型I Cカードと非接触型I Cカードの両方の機能を有するI Cカードの構成の例を示す第2の図である。

【図12】図12は、接触型I Cカードと非接触型I Cカードの両方の機能を有するI Cカードの構成の例を示す第3の図である。

【符号の説明】

1, 2, 3, 4…I Cカード

1 1…非接触I /F部

1 2…接触I /F部

1 3…非接触回路部

1 3 1…信号処理部

1 3 2…暗号化部

1 3 3…署名処理部

1 3 4…認証処理部

1 3 5…メモリ

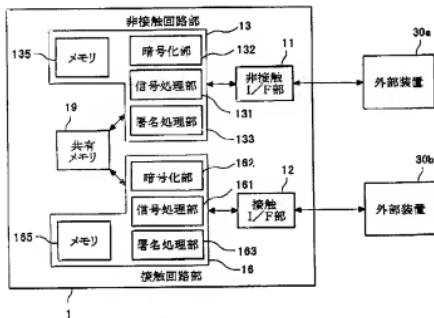
1 6…接触回路部

1 6 1…信号処理部

162…暗号化部
163…署名処理部
164…認証処理部
165…メモリ

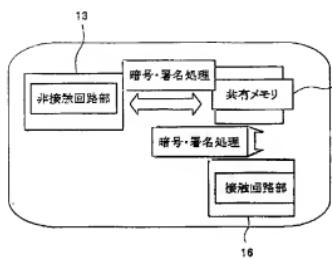
19…共有メモリ
20…データ転送部
17…メモリ
30…外部装置

【図1】

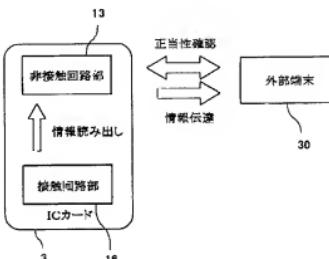


1

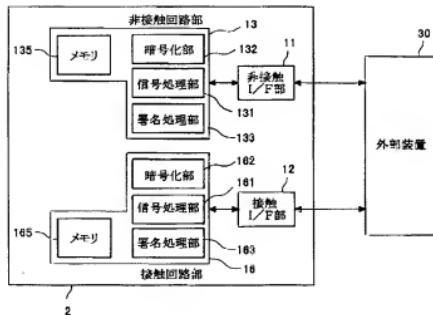
【図2】



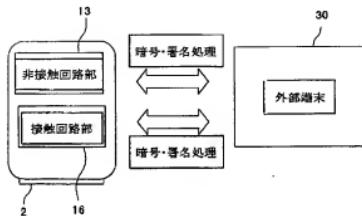
【図6】



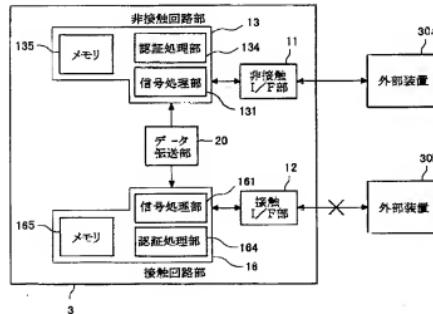
【図3】



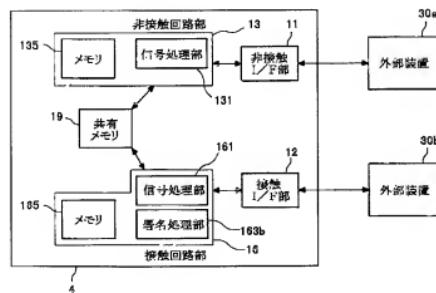
【図4】



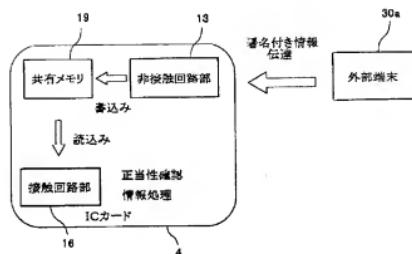
【図5】



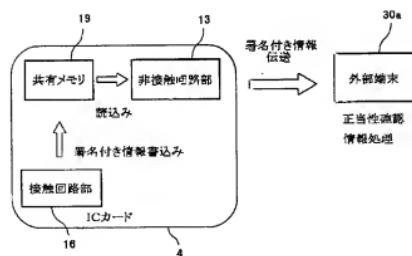
【図7】



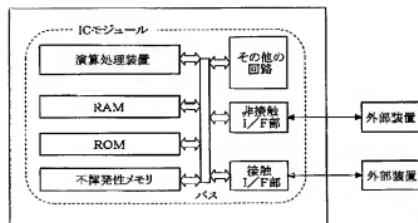
【図8】



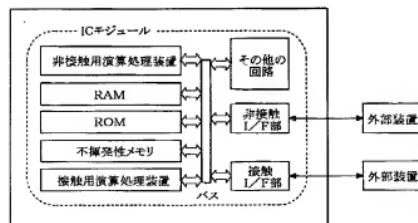
【図9】



【図10】



【図11】



【図12】

